UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/677,660	10/02/2003	Susann Marie Keohane	AUS920030640US1	9966

60501 7590 07/17/2008
LENOVO COMPANY
c/o BIGGERS & OHANIAN, LLP
P.O. BOX 1469
AUSTIN, TX 78767-1469

EXAMINER	
PHAN, TUANKHANH D	
ART UNIT	PAPER NUMBER
2163	
MAIL DATE	DELIVERY MODE
07/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/677,660	KEOHANE ET AL.	
	Examiner	Art Unit	
	TUAN-KHANH PHAN	2163	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 April 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

Response to Amendment

The amendment, filed 4/22/2008, has been entered and acknowledge by the Examiner. Claims 1-39 are pending.

Response to Arguments

Applicant's arguments, filed 4/22/2008, have been fully considered but they are not persuasive.

Issue I. The Applicant argues that measures Herrero's secure communication between entities does not disclose monitoring the type of connection between a computer and a network in a current computing environment as claimed in the present application. In fact, Herrero does not disclose monitoring at all. Herrero at the cited reference point only discloses determining whether security measures needed for a particular communication exist. Examples of monitoring as claimed in the present application include periodically determining the type of connection between a computer and a network and an event-driven determination of the type of connection between a computer and a network carried out each time the TCP/IP client on a computer runs during the computer's power-up procedure. Additionally, Applicants note that at no point in the entire reference does Herrero mention the terms 'monitor' or 'monitoring.' The secure communication between entities consisting of determining whether security measures are needed, establishing security measures if they are needed but do not exist, and initiating communication of Herrero therefore neither discloses nor suggests monitoring the type of connection between a computer and a network in a current computing environment as claimed in the present application.

Response I. The Examiner would like to assert that determining and checking the necessary security needs for communication between entities in the same network or different networks (p. 4, lines 13-15) are equivalent to monitoring a connection between a computer and a network, as claimed in the present application. In addition, different types of communication connections are available in Herrero (at least p. 10, lines 1-2). Thus, Applicant's argument is not persuasive.

Issue II. The Applicant argues that Holden neither discloses nor suggest sending data from a buffer when a computer is connected to a changed computer environment having a new type of connection that has the security level required for the data.

Response II. The Examiner would like to point that having a waiting queue to hold data until a secured line of communication is available, and then data allowed to proceed/send is no difference than having a buffer, as claimed by the present application, then sending data when the connection has changed and the security level required for the data has met. Thus, Applicant's argument is not persuasive.

Issue III. The Applicant argues that Herrero neither discloses nor suggests connecting a computer to a network in a second computer environment, wherein the second computer environment has the security control required for a specified security level.

Response III. As disclosed by Herrero (p. 4, lines 13-15), different network environments is being checked accordingly with the security level needed based on data being transmitted and the security control required. A plurality of different network connections established among entities encompasses “the second computing environment,” as claimed by the present application, and more. Thus, Applicant’s argument is not persuasive.

Issue IV. The Applicant argues that Ueda neither discloses nor suggests sending data from a buffer when a computer is connected to a changed computer environment having a new type of connection that has the security required for the data.

Response IV. The Examiner would like to state that, at least in col. 3, lines 36-40, having a buffer means for storing data there until security level of the network and user required are met reads on the limitation, “sending data from a buffer when a computer is connected to a changed computer environment having a new type of connection that has the security required for the data” as recited by the present application because the buffer provided by Ueda functions no difference than as claimed by the applicant. Thus, Applicant’s argument is moot.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herrero et al. (WO 00/74345), hereinafter Herrero, in view of Holden et al. (US Pat. 5,828,832), hereinafter Holden.

Regarding claims 1, 14 and 27, Herrero discloses a method/system for providing a necessary level of security for a computer capable of connecting to different computing environments are determined (i.e. **providing security requirements for establishment between entities in one or more networks and determining the needed security levels for data and connections**, abstract), the method comprising:

monitoring a type of connection between the computer and a network in a current computing environment (i.e. **measuring security for connection exist between entities – e.g. a computer and its network,** p. 4 lines 5-10);

determining a security level of data before sending the data across the network (i.e. **determine the security level needed based on the information, data, being transmitted,** p. 4, lines 13-14);

but Herrero does not explicitly teach storing the data in a buffer instead of sending the data across the network if the connection to the network lacks a security control required for the determined security level of the data; and sending the data from the buffer.

However, in the same field of endeavor, Holden discloses storing the data in a buffer (i.e. **storing the datagram/data, in the waiting queue/buffer, col. 11, lines 28-30**), instead of sending the data across the network if the connection to the network lacks a security control required for the determined security level of the data (i.e. **then**

waiting to be sent across the network upon exchanged and met security requirements – association grant message received, col. 11, lines 30-31); and

Holden discloses sending the data from the buffer when the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data (i.e. **upon the verification of connection/receiver and security control required for the datagram is validated, datagram is sent from the queue/buffer, col. 11, lines 50-52**).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the waiting buffer for data security taught by Holden into the verification of connection security taught by Herrero to allow the operations of computer network entities transmitting secured data across the network with out any expensive network security interfaces (Holden).

Regarding claims 2, 15 and 28, Herrero and Holden disclose the method of claims 1, 14 and 27, and Holden further discloses wherein monitoring a type of connection comprises periodically determining the type of connection between the computer and the network (i.e. the procedure of checking destination network connection is repeated/periodically, col. 19, lines 13-14).

Regarding claims 3, 16 and 29, Herrero and Holden disclose the method of claims 1, 14 and 27, Holden further discloses wherein monitoring a type of connection comprises event-driven determining of the type of connection between the computer and the network (i.e. **processing based on an anticipated event is equivalent to event-driven determination**, col. 16, lines 56-57).

Regarding claims 4, 17 and 30, Herrero and Holden disclose the method of claims 3, 16 and 29, Holden further discloses wherein the steps of the method are carried out by a software process and event-driven determining of the type of connection is carried out whenever the process is invoked (col. 16, lines 56-57).

Regarding claims 5, 18 and 31, Herrero and Holden disclose the method of claims 3, 16 and 29, wherein determining a security level results in a determination that data to be transmitted requires at least some level of security and event-driven determining of the type of connection is carried out in response to such determination (see the discussions of level of security of data in claim 1 and event-driven in claim 3).

Regarding claims 6, 19 and 32, Herrero and Holden disclose the method of claims 1, 14 and 27, Herrero further discloses wherein determining a security level of data before sending the data across the current network comprises reading the security level of data from a markup element embedded in the data (i.e. markup element embedded in the data is a form of applying data encryption or data masking, p. 6, lines 15-17).

Regarding claims 7, 20 and 33, Herrero and Holden disclose the method of claims 1, 14 and 27, Holden further discloses wherein determining a security level of data before sending the data across the current network comprises reading the security level of data from meta-data in a header in a network message (IP datagrams, e.g. IP header, is a type of meta-data, col. 16, line 56).

Regarding claims 8, 21 and 34, Herrero and Holden disclose the method of claims 1, 14 and 27, Herrero further discloses comprising returning a non-fatal error to a sending program if the connection to the network lacks a security control required for the data (enable looping, Figure 7, allows a future or alternative checking such that non-fatal error is considered).

Regarding claims 9, 22 and 35, Herrero and Holden disclose the method of claims 8, 21 and 34, Holden discloses further comprising the sending program's informing a user that the data will be held in a security buffer until the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data (i.e. **storing the datagram/data, in the waiting queue/buffer, col. 11, lines 28-30**, **then waiting to be sent across the network upon exchanged and met security requirements – association grant message received, col. 11, lines 30-31**).

Regarding claims 10, 23 and 36, Herrero and Holden disclose the method of claims 8, 21 and 34, Herrero discloses further comprising the sending program's prompting a user with the option to create a secure tunnel for transmission of the data (security level needed may be determined, p. 4, lines 10-13).

Regarding claims 11, 24 and 37, see discussion of claims 1 above, Herrero further discloses a method for providing a necessary level of security for a computer capable of connecting to different computing environments, the method comprising:

connecting the computer to a network in a first computing environment determined (i.e. **providing security requirements for establishment between entities in one or more networks and determining the needed security levels for data and connections**, abstract);

specifying a security level for data to be sent across the network (abstract);

instructing a sending program to send the data across the network (abstract);

receiving an indication that security control of the first computing environment lacks a security control required for the specified security level (p. 4, lines 5-20);

connecting the computer to the network in a second computing environment, wherein the second computing environment has the security control required for the specified security level (p. 4, lines 5-20); and

receiving an indication that the data has been sent across the network (p. 10, lines 25).

Regarding claims 12, 25 and 38, Herrero and Holden disclose the method of claims 11, 24 and 37, Herrero further discloses comprising: determining, when the computer is connected to the second network, that the second computing environment has the security control required for the specified security level (i.e. **providing security requirements for establishment between entities in one or more networks and determining the needed security levels for data and connections**, abstract); and

automatically sending the data across the network promptly upon determining that the second computing environment has the security control required for the specified security level (abstract).

Regarding claims 13, 26 and 39, Herrero and Holden disclose the method of claims 11, 24 and 37, Herrero further discloses comprising: receiving an indication that the second computing environment has the security control required for the specified security level (p. 4); and again instructing the sending program to send the data across the network (Figure 7, “770”).

Claims 1, 14 and 27 are also rejected **under 35 U.S.C. 103(a)** as being unpatentable over Herrero et al. (WO 00/74345), hereinafter Herrero, in view of Ueda (US Pat. 5,692,179).

Regarding claims 1, 14 and 27, Herrero discloses a method/system for providing a necessary level of security for a computer capable of connecting to different computing environments are determined (i.e. **providing security requirements for establishment between entities in one or more networks and determining the needed security levels for data and connections**, abstract), the method comprising:

monitoring a type of connection between the computer and a network in a current computing environment (i.e. **measuring security for connection exist between entities – e.g. a computer and its network,** p. 4 lines 5-10);

determining a security level of data before sending the data across the network (i.e. **determine the security level needed based on the information, data, being transmitted,** p. 4, lines 13-14);

but Herrero does not explicitly teach storing the data in a buffer instead of sending the data across the network if the connection to the network lacks a security control required for the determined security level of the data; and sending the data from the buffer.

However, in the same field of endeavor, Ueda discloses storing the data in a buffer (i.e**. data are temporarily stored to the buffer means**, col. 4, lines 60-62) instead of sending the data across the network if the connection to the network lacks a security control required for the determined security level of the data (col. 4, lines 60-62); and

Ueda discloses sending the data from the buffer when the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data (i.e. **and then transmitted when security level of the connection and security level of data are in conformity**, col. 4, lines 59-62).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the waiting buffer for data security taught by Ueda into the connection security taught by Herrero to allow the operations of computer network entities transmitting secured data across the network instantly upon registration of security network by another user (Ueda).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TUAN-KHANH PHAN whose telephone number is (571)270-3047. The examiner can normally be reached on 4/5/9.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Don Wong can be reached on 571-272-1834. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TKP
/Hung T Vy/
Primary Examiner, Art Unit 2163